ETSI GR ISC 004 V1.1.1 (2026-02)

GROUP REPORT

Integrated Sensing And Communications (ISAC); Security, Privacy, Trustworthiness and Sustainability

Disclaimer

The present document has been produced and approved by the Integrated Sensing And Communications (ISAC) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG.
It does not necessarily represent the views of the entire ETSI membership.

Reference
DGR/ISC-004

Keywords
ISAC, privacy, security, sustainability, trustworthiness

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights 6
Foreword 6
Modal verbs terminology 6
Executive summary 6
Introduction 7
1 Scope 8
2 References 8
2.1 Normative references 8
2.2 Informative references 8
3 Definition of terms, symbols and abbreviations 10
3.1 Terms 10
3.2 Symbols 10
3.3 Abbreviations 10
4 Definitions and foundations for security, privacy, trustworthiness, and sustainability 11
4.1 System terminology for ISAC-enabled 6G systems 11
4.2 Security 12
4.3 Personal Identifiable Information (PII) 12
4.4 Privacy 12
4.5 Trustworthiness 12
4.6 Sensing policy, sensing consent and sensing transparency 13
4.6.1 Sensing policy 13
4.6.2 Sensing consent 13
4.6.3 Sensing transparency 13
4.7 Sustainability 13
4.8 Types of Sensing Targets in ISAC-Enabled 6GS 13
5 Key issues on security and privacy 14
5.1 Key issue #1: Use of 6GS for unauthorized sensing 14
5.1.1 Key issue details 14
5.1.2 Security, privacy, and trustworthiness threats 15
5.1.3 Potential requirements and metrics 16
5.2 Key issue #2: Use of sensing signals by the target for data eavesdropping 18
5.2.1 Key issue details 18
5.2.2 Security, confidentiality, and trustworthiness threats 18
5.2.3 Potential requirements and metrics 19
5.3 Key issue #3: Over-the-air manipulation of 6G RF sensing signals 19
5.3.1 Key issue details 19
5.3.2 Security, privacy, and trustworthiness threats 19
5.3.3 Potential requirements and metrics 20
5.4 Key issue #4: Secure handling of sensing data 20
5.4.1 Key issue details 20
5.4.2 Security, privacy, and trustworthiness threats 20
5.4.3 Potential requirements and metrics 20
5.5 Key issue #5: Integrity of ISAC-enabled 6GS entities, and immutability of sensing data or sensing results 21
5.5.1 Key Issue details 21
5.5.2 Potential threats 21
5.5.3 Potential requirements and metrics 21
5.6 Key issue #6: Sensing privacy, confidentiality, and consent in non-public spaces 21
5.6.1 Key issue details 21
5.6.2 Security, privacy, and trustworthiness threats 21
5.6.3 Potential requirements and metrics 22
5.7 Key issue #7: Privacy issues related to consent and transparency 22

5.7.1 Key issue details 22
5.7.2 Security, privacy, and trustworthiness threats 22
5.7.3 Potential new requirements 23
5.8 Key issue #8: Privacy-related aspects regarding sensing of humans that are not connected to the 6GS 23
5.8.1 Key issue details 23
5.8.2 Security, privacy, and trustworthiness threats 23
5.8.3 Potential requirements and metrics 23
5.8.4 Potential regulatory requirements 23
5.9 Key issue #9: Privacy-related aspects regarding sensing of humans that are connected to the 6GS 24
5.9.1 Key issue details 24
5.9.2 Security, privacy, and trustworthiness threats 24
5.9.3 Potential requirements and metrics 24
5.9.4 Potential regulatory requirements 24
5.10 Key issue #10: Unauthorized passive 6G RF sensing 24
5.10.1 Key issue details 24
5.10.2 Security, privacy, and trustworthiness threats 25
5.10.3 Potential requirements and metrics 25
5.11 Key issue #11: Authorization of ISAC-enabled 6GS entities 25
5.11.1 Key Issue details 25
5.11.2 Potential threats 25
5.11.3 Potential requirements and metrics 25
5.12 Key issue #12: Privacy-related aspects regarding UE positioning in sensing 25
5.12.1 Key issue details 25
5.12.2 Security, privacy, and trustworthiness threats 26
5.12.3 Potential requirements and metrics 26
5.13 Key issue #13: Privacy risks from heterogeneous sensing capabilities 26
5.13.1 Key issue details 26
5.13.2 Security, privacy and trustworthiness threats 26
5.13.3 Potential new requirements 26
5.14 Key issue #14: Privacy-related aspects of AI-based sensing data processing 27
5.14.1 Key issue details 27
5.14.2 Security, privacy, and trustworthiness threats 27
5.14.3 Potential requirements and metrics 27
5.15 Key issue #15: Privacy challenges and malicious attacks in cooperative sensing 27
5.15.1 Key issue details 27
5.15.2 Security, privacy, and trustworthiness threats 28
5.15.3 Potential requirements and metrics 28

6 Considerations and consolidation for privacy, security, and trustworthiness 28
6.1 Considerations on sensing data ownership and accountability in ISAC System 28
6.2 Considerations for trustworthiness 29
6.3 Consolidated Potential Functional Requirements 29

7 Key issues on sustainability 31
7.1 Key issue #1: Power consumption of ISAC-enabled 6GS 31
7.1.1 Key issue details 31
7.1.2 Potential requirements and metrics 32
7.2 Key issue #2: Utilization of spectrum resources in ISAC-enabled 6GS 32
7.2.1 Key issue details 32
7.2.2 Potential requirements and metrics 32
7.3 Key issue #3: Overall environmental system footprint of ISAC-enabled 6GS 32
7.3.1 Key issue details 32
7.3.2 Potential requirements and metrics 33
7.4 Key issue #4: Considerations on 'good health and well-being' with ISAC-enabled 6GS 33
7.4.1 Key issue details 33
7.4.2 Potential requirements and metrics 34

8 Considerations and consolidation on sustainability 34
8.1 High-level objectives for sustainability 34

9 Conclusion 34

Annex A: Mapping of security and privacy key issues to use cases of ETSI GR ISC 001 36

Annex B: Mapping of sustainability key issues to use cases of ETSI GR ISC 001.....39
History 41

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI IPR online database.

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Group Report (GR) has been produced by ETSI Industry Specification Group (ISG) Integrated Sensing And Communications (ISAC).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Executive summary

The present document provides a comprehensive study on aspects related to security, privacy, trustworthiness, and sustainability within the context of Integrated Sensing and Communications (ISAC).

The present document identifies 19 key issues, of which 15 are related to privacy and security, and 4 related to sustainability. For each key issue, a detailed description is provided, together with potential technical and non-technical requirements. For the privacy and security key issues, the analysis is supported with a comprehensive set of threats per key issue.

In addition, the present document includes initial considerations on aspects related to trustworthiness and ownership of sensing data. The potential technical and non-technical requirements are analysed to identify consolidated requirements that future 6G systems should meet to deploy secure, privacy-preserving, trustworthy, and sustainable ISAC services.

Introduction

Interest in ISAC is growing worldwide among standardization bodies, industrial stakeholders, academia, and numerous collaborative projects. In this context, the present document provides a study on challenges related to security, privacy, trustworthiness, and sustainability for enablement of ISAC in a future 6G System.

1 Scope

The scope of the present document is to study security, privacy, trustworthiness, and sustainability in the context of ISAC in a future 6G System. This includes:

- An overview of existing definitions and characterizations of security, privacy, trustworthiness, and sustainability, and identification of related terms.
- Identification of key issues, description of relevant threats, and definition of potential requirement for security and privacy.
- Identification of key issues on sustainability.
- Consolidation of potential requirements corresponding to the key issues on security and privacy.
- Additional considerations regarding trustworthiness and data ownership.
- High-level objectives for sustainability.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long-term validity.

The following referenced documents may be useful in implementing an ETSI deliverable or add to the reader's understanding, but are not required for conformance to the present document.

[i.1] ETSI GR ISC 001 (V1.1.1): "Integrated Sensing And Communications (ISAC);Use Cases and Deployment Scenarios".

[i.2] ISO/IEC 23643:2020: "Software and systems engineering — Capabilities of software safety and security verification tools".

[i.3] ISO/IEC TS 5723:2022(en): "Trustworthiness Vocabulary", 2025.

[i.4] ISO 20252:2019: "Market, opinion and social research, including insights and data analytics — Vocabulary and service requirements".

[i.5] ETSI TR 121 905 (V18.0.0): "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; Vocabulary for 3GPP Specifications (3GPP TR 21.905 version 18.0.0 Release 18)".

[i.6] ISO 7498-2:1989: "Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture".

[i.7] ISO/IEC 20000-10:2018: "Information technology - Service management - Part 10: Concepts and vocabulary".

[i.8] NIST SP 800-12: "An introduction to computer security: the NIST handbook", 1995.

[i.9] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[i.10] ISO TS 27790:2009: "Health informatics — Document registry framework".

[i.11] ISO TS 14441:2013: "Health informatics — Security and privacy requirements of EHR systems for use in conformity assessment".

[i.12] NIST SP 800-160v1r1: "Engineering Trustworthy Secure Systems".

[i.13] Gro Harlem Brundtland: "Report of the World Commission on Environment and Development: Our Common Future" 1987.

[i.14] ISO/IEC 29100:2020-03: "Information technology - Security techniques - Privacy framework".

[i.15] NIST SP 800-122 E. McCallister, T. Grance, K. Scarfone: "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)".

[i.16] 3GPP TR 22.837 (V19.4.0): "Feasibility Study on Integrated Sensing and Communication (Release 19)".

[i.17] Nyangaresi, V.O., Abduljabbar, Z.A., Mutlaq, K.AA., Hussain, M.A., Hussien, Z.A.: "Forward and Backward Key Secrecy Preservation Scheme for Medical Internet of Things", 2023.

[i.18] Mozilla™ Foundation: "Immutable", 2025.

[i.19] Goetz et al.: "Java Concurrency in Practice; Section 3.4. Immutability", Addison Wesley Professional, 2006.

[i.20] P. Dass, S. Ujjwal, J. Novotny, Y. Zolotavkin, S. Köpsell: "Addressing privacy concerns in joint communication and sensing for 6G networks: challenges and prospects", Privacy Technologies.

[i.21] R. Becker et al.: "DAISY: A data information system for accountability under the general data protection regulation", GigaScience, 8(12), giz140.

[i.22] European Commission: "Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment".

[i.23] ETSI TR 128 908 (V18.0.0): "5G; Study on Artificial Intelligence/Machine Learning (AI/ ML) management (3GPP TR 28.908 version 18.0.0 Release 18)".

[i.24] European Commission: "Draft standardisation request as regards European Trusted Data Framework", 2024.

[i.25] ETSI TR 104 177: "Data Solutions (DATA); Landscape of Relevant Standards and Technologies for Data".

[i.26] ETSI TR 104 180: "Data Solutions (DATA); Development and identification of Data Quality Metrics".

[i.27] Draft CWA for comment CENELEC: "Trusted Data Transaction - Part 2: Trustworthiness requirements", 2025.

[i.28] Assaf Kasher, Yingxiang Sun: "Wifi-Sensing-Use-Cases", IEEE 802.11™ WLANs WG Group Mentor Public Documentation Portal, Group TGbf, DCN 1712, Rev 2, 2020.

[i.29] United Nations: "Sustainable Development Goals and the 2030 Agenda: Why Environmental Sustainability and Gender Equality are so important to Reducing Poverty and Inequalities - UNEP Perspectives Issue No. 17", 2015.

[i.30] ETSI GR ISC 003: "Integrated Sensing And Communications (ISAC); System and RAN Architectures".

3 Definition of terms, symbols and abbreviations

3.1 Terms

Void.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

3GPP	3rd Generation Partnership Project
6GS	6th Generation System
AF	Application Function
AI	Artificial Intelligence
BLER	Block Error Rate
BS	Base Station
CEN	European Committee for Standardization
CN	Core Network
CPR	Consolidated Potential Requirement
CPU	Central Processing Unit
CWA	CEN Workshop Agreement
EC	European Commission
ETSI	European Telecommunications Standards Institute
GDPR	General Data Protection Regulation
ISAC	Integrated Sensing and Communication
KPI	Key Performance Indicator
ML/AI	Machine Learning/ Artificial Intelligence
NF	Network Function
PII	Personally Identifiable Information
PR	Potential Requirement
PRR	Potential Regulatory Requirement
RAN	Radio Access Network
RF	Radio Frequency
RRC	Radio Resource Control
SA3	subcommittee on Security (3GPP)
SBA	Service Based Architecture
SIDP	Sensing Input Data Producer
SLA	Service Level Agreement
TC DATA	Technical Committee Data Solutions
TC	Technical Committee
TR	Technical Report
TSSA	Target Sensing Service Area
UAV	Unmanned Aerial Vehicle
UC	Use Case
UE	User Equipment
UN	United Nations
XR	Extended Reality

4 Definitions and foundations for security, privacy, trustworthiness, and sustainability

4.1 System terminology for ISAC-enabled 6G systems

For the purposes of the present document, the following terms as defined in ETSI GR ISC 003 [i.30] apply:

- **6GS Sensing Service Consumer (SSC):** a 6GS entity which can be authorized to request and consume 6G Sensing Service(s). SSC may include UEs, Access Nodes, and Core Network Functions.
- **3rd party Sensing Service Consumer (3-SSC):** an entity, not part of 6GS, which can be authorized to request and consume 6G Sensing Service(s).
- **Sensing signal:** is a transmitted signal from a sensing transmitter for the purpose of sensing. The signal can be 6G or non-6G.
- A **sensing transmitter:** is a 6G or non-6G entity that transmits a sensing signal.
- A **sensing receiver:** is a 6G or non-6G entity that receives a sensing signal and produces sensing data. A sensing receiver can be co-located with a sensing transmitter.
- **Sensing data:** is the 6G or non-6G data produced for sensing purposes.
- **A sensing entity:** is an entity referring to a sensing transmitter or to a sensing receiver.
- A **sensing service:** is a feature of the 6GS that is offered to service consumers. A sensing service provides sensing results based on communicated requirements and KPIs.
- **Sensing function:** indicates the logical function, which is involved to support a Sensing Service.

NOTE 1: The sensing function cannot be a sensing entity.

- A **sensing task:** is communicated from a sensing function to sensing entities and functions and consists of configuration information of the required sensing transmitter(s) and sensing receiver(s) (if applicable), the collection of sensing data, the processing of the sensing data and the exposure of the sensing results. Each sensing task fulfils a Sensing Service request.
- A **Target Sensing Service Area (TSSA):** is defined as a cartesian location area that needs to be sensed by deriving characteristics of the environment and/or objects within the environment with certain sensing service quality from the impacted (e.g. reflected, refracted, diffracted) 6G or non-6G sensing signals. This includes both indoor and outdoor environments.
- The **sensing results:** are processed or non-processed sensing data which may include characteristics of objects (e.g. type, distance, velocity, trajectory, size, shape, material), or other contextual information (e.g. time of generation, environmental information) about objects in the Target Sensing Service Area.

NOTE 2: It is not precluded that the sensing result exposed to an entity within 6GS or to a authorized third party may in some cases consist of the sensing data itself.

- **Sensing contextual information:** is information that is exposed with the sensing results which provides context to the conditions under which the sensing results were derived (e.g. time of generation, environmental information). This information does not contain sensing data or sensing results.
- **Fusion:** refers to a process to join two or more streams of sensing data or sensing results together to form one or more sensing data or sensing result stream(s). Fusion can take place at the origin of the sensing data, along the system entities of a 6GS. The fusion of sensing results can also take place along all 6GS system entities. Fusion can also take place in non-6GS entities.

4.2 Security

General definition: Security refers to the resistance to intentional, unauthorized action(s) intended to harm or compromise a system, see ISO/IEC 23643 [i.2]. This involves preserving the properties such as confidentiality, integrity and availability of information as defined in ISO 20252 [i.4] and ETSI TR 121 905 [i.5].

Confidentiality: This property ensures that data is not made available or disclosed to unauthorized individuals, entities, or processes as defined in ISO 7498-2 [i.6].

Integrity: This property ensures that data has not been altered or destroyed in an unauthorized manner as defined in ISO 7498-2 [i.6] and ETSI TR 121 905 [i.5].

Availability: This property ensures that data is accessible and usable upon demand by an authorized entity, as defined in ISO 7498-2 [i.6]. It may further ensure the ability of a system to offer a service at an agreed time or over an agreed period of time, see ISO/IEC 20000-10 [i.7] and NIST SP 800-12 [i.8].

Based on the definitions in ISO/IEC 23643 [i.2], ISO 20252 [i.4], ETSI TR 121 905 [i.5], ISO 7498-2 [i.6], ISO/IEC 20000-10 [i.7] and NIST SP 800-12 [i.8].

Security in the context of ISAC refers to the resilience of integrated sensing and communication systems against intentional, unauthorized actions intended to harm or compromise system operations. This encompasses the preservation of confidentiality, integrity, and availability of both communication and sensing information, systems, and services such as sensing data, sensing entities, and sensing functions.

4.3 Personal Identifiable Information (PII)

As defined by EU GDPR [i.9], **Personally Identifiable Information** (PII) means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Even information that is not identifiable on its own can be considered **sensitive data**, if it may become identifiable when joined with other datasets.

4.4 Privacy

General definition: Privacy refers to the freedom to remain free from intrusions into one's personal life or affairs, particularly when such intrusions result from the improper or unlawful collection and use of personal data as defined in ISO TS 27790 [i.10]. Privacy covers the rights and obligations of individuals and organizations regarding the collection, use, storage, sharing, and disposal of PII, see ISO TS 14441 [i.11]. Privacy is always related to personal data or PII.

NOTE: While confidentiality focuses on preventing the disclosure of information to unauthorized actors, privacy specifically deals with the confidentiality of PII, including its management during collection, use, storage, sharing, and disposal. Therefore, privacy is not the same as confidentiality.

Based on the definitions in ISO TS 27790 [i.10] and information in ISO TS 14441 [i.11].

Privacy in the context of ISAC refers to the protection of individuals' personal information in integrated sensing and communication systems, focusing on the responsible collection, use, retention, disclosure, and disposal of PII, obtained through both communication and sensing activities. It ensures that individual data is handled ethically and transparently, safeguarding against illegal data gathering, usage, and inferences while respecting individual data protection rights and guidelines.

4.5 Trustworthiness

General definition: Trustworthiness as defined in ISO/IEC TS 5723 [i.3] refers the ability of the system to meet the expectations of the stakeholders in a measurable and verifiable way. Trustworthiness covers many different trustworthiness characteristics such as accountability, accuracy, authenticity, availability, integrity, privacy, quality, safety, security, sustainability, transparency and usability.